



Цифровые следы в расследовании преступлений, совершенных с использованием возможностей интернет-рынка Форекс

И. Е. Реуцкая

*Всероссийский научно-исследовательский институт
Министерства внутренних дел Российской Федерации, Москва, Россия
irinareutskaya@yandex.ru*

Аннотация. Статья посвящена вопросам изучения цифровых следов от преступлений, совершенных с использованием возможностей межбанковского валютного интернет-рынка Форекс. Исследование данного вопроса проводилось с применением системного, логического, формально-юридического методов, методов анализа и синтеза. Результаты исследования позволили показать, что цифровыми следами от преступлений, совершенных с использованием возможностей межбанковского валютного интернет-рынка Форекс, является информация с фальшивых сайтов, со счетов (например, торговых) потерпевшего и третьих лиц.

Ключевые слова: преступление, цифровые следы, экономика, интернет-рынок Форекс, сайт, компьютерная программа, торговая биржа, преступные схемы

Для цитирования: Реуцкая И. Е. Цифровые следы в расследовании преступлений, совершенных с использованием возможностей интернет-рынка Форекс // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2024. Вып. 2 (851). С. 135–139.

Original article

Digital Traces in the Investigation of Crimes Committed Using the Opportunities of the Online Forex Market

Irina E. Reutskaya

*All-Russian Research Institute of the Ministry of Internal Affairs of the Russian Federation, Moscow, Russia
irinareutskaya@yandex.ru*

Abstract. The article is devoted to the study of digital traces of crimes committed using the opportunities of the interbank online Forex currency market. The study of this issue was carried out using systematic, logical, formal legal methods, methods of analysis and synthesis. The results of the study allowed us to show that the digital traces of crimes committed using the opportunities of the interbank online Forex currency market are information from fake websites, from accounts (for example, trading) of the victim and third parties.

Keywords: crime, digital traces, economy, online Forex market, website, computer program, trading exchange, criminal schemes

For citation: Reutskaya, I. E. (2024). Digital traces in the investigation of crimes committed using the opportunities of the online Forex market. Vestnik of Moscow State Linguistic University, 2(851), 135–139.

ВВЕДЕНИЕ

Современный этап развития общества характеризуется появлением новых способов реализации экономической деятельности, основной отличительной особенностью которой является осуществление в информационной среде иногда даже при отсутствии каких-либо документов на бумажном носителе, подтверждающих совершение тех или иных сделок и, соответственно, наличие «бумажных» гражданско-правовых договоров по ним. Контракты оформляются в электронном виде, подписываются электронной подписью или ее усиленным вариантом, то есть заключаются дистанционно. Все чаще – это самоисполняющиеся смарт-контракты, которые после нажатия кнопки «согласен» на клавиатуре компьютера или на ином устройстве с выходом в информационно-телекоммуникационную сеть Интернет (далее – Интернет) отменить не представляется возможным. В некоторых случаях предметом вышеуказанных договоров являются финансовые инструменты, которые существуют только в виртуальном мире, поскольку создаются на информационных платформах или в информационных системах, хранятся на них, переходят к другим владельцам на основании договоров купли-продажи, дарения, по наследству и т. д. и прекращают свое существование (погашаются). Вместе с тем эти инструменты имеют под собой вполне материальную основу (например, акции «Атомайз» – это цифровые финансовые активы, привязанные к драгоценным металлам, алмазам и др.).

Новые формы ведения бизнеса и интернет-среда как место его реализации, с одной стороны, создают возможности для его развития, а с другой – влекут создание новых сложных схем совершения преступлений в сфере экономики, которые обуславливают трудности в их расследовании.

О ПОНЯТИИ «ЦИФРОВЫЕ СЛЕДЫ»

Многие из преступлений рассматриваемой категории совершаются с применением информационных технологий, что обуславливает появление от них так называемых цифровых следов. С точки зрения Е. Р. Россинской и И. А. Рядовского цифровым следом является «криминалистически значимая компьютерная информация о событиях и действиях, отраженная в материальной среде, в процессе ее возникновения, обработки, хранения и передачи» [цит. по: Захарова, Шкатулов, 2023].

Данная информация (цифровой след) «может состоять из большого количества отдельных информационных элементов, которые могут быть

записаны как на одном, так и на нескольких электронных носителях информации, подключенных как к одному, так и к нескольким компьютерам, объединенным в информационную систему или информационно-телекоммуникационную сеть» [Романова, 2003]. Таким образом, цифровые следы могут быть образованы и вне Интернета, а содержаться только на каком-либо электронном носителе информации. К таким цифровым следам относятся, например, бухгалтерские документы [Буйнов, 2022]. Исходя из вышеизложенного можно сделать вывод, что в настоящее время при расследовании всех преступлений в сфере экономики требуется поиск их цифровых следов. Вместе с тем некоторые преступления совершаются непосредственно в информационных системах, а значит содержащаяся в них цифровая информация является ключом к расследованию таких преступных деяний. К указанным преступлениям относятся совершенные с использованием возможностей межбанковского валютного интернет-рынка Форекс.

СХЕМЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ВОЗМОЖНОСТЕЙ МЕЖБАНКОВСКОГО ВАЛЮТНОГО ИНТЕРНЕТ-РЫНКА ФОРЕКС

Проведенный анализ судебной практики рассмотрения указанной категории уголовных дел позволил выявить три основные преступные схемы совершения преступлений.

Схема № 1 – заключается в имитации торговли на бирже (рис. 1).

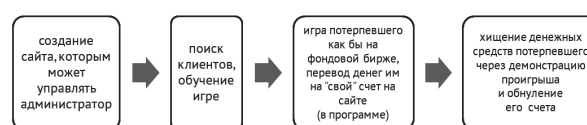


Рис. 1. Хищение денежных средств потерпевших посредством имитации игры на межбанковском валютном интернет-рынке Форекс

В данном случае потерпевшие «играли на валютных парах» в специальной программе «Метатрейдер» или на специально созданном сайте. При этом котировки устанавливал преступник как администратор программы / сайта. Они не обязательно должны были соответствовать котировкам на реальном валютном рынке. Денежные средства потерпевших за пределы программы / сайта не выходили и на официальные валютные рынки не поступали. Администратор программы / сайта имел возможность управлять игрой «на бирже»,

например, создавать различные помехи в ходе игры, изменять котировки с целью закрытия сделки с убытком потерпевшего, удалять сведения из программы. Деньги клиента на счет компании вносились не самим потерпевшим, а иным лицом, имеющим код доступа к данной программе / сайту. При этом у потерпевшего создавалось впечатление, что его денежные средства внесены на принадлежащий ему счет, поскольку их баланс отражался на экране компьютера.

Так, например, при открытии клиентами компании Arena Markets Limited (Арена Маркетс Лимитед) счетов на сайтах www.arenafox.net, www.arena-forex.ru, рынка Форекс, сайтов и перечислении на них денежных средств они отражались на странице в личном кабинете клиентов, с целью создания ложной убежденности о поступлении на счета, с которых якобы осуществляется торговля на рынке Форекс¹.

В данном случае к цифровым следам преступления относится информация с сайта о котировках и их изменениях, о балансе кошельков клиентов и движении денежных средств на них.

Схема № 2 – торговля на бирже с обязательным перечислением денежных средств на счет, открытый на имя лица, совершившего преступление (рис. 2).

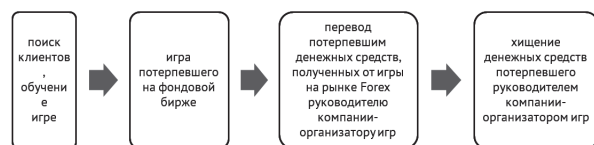


Рис. 2. Хищение денежных средств потерпевших, полученных от сделок на межбанковском валютном интернет-рынке Форекс

В рассматриваемом случае происходит хищение денежных средств клиента, перечисленных им на определенные цели.

Так, например, Ф., с целью осуществления сделок купли-продажи на международном рынке с привлечением денежных средств инвесторов подготовил Соглашение об участии в долевом инвестиционном управлении (далее – Соглашение), согласно которому клиенты выступали в качестве инвесторов, то есть лиц, открывающих торговые счета и вносящих на них денежные средства для перевода на счет долевого инвестиционного управления. Ф. выступал в качестве управляющего, то есть физического лица, осуществляющего торговые операции на счету долевого инвестиционного управления в соответствии

с условиями данного Соглашения. Согласно выше-названному Соглашению инвестор путем перевода предоставляет Ф. в управление денежные средства со своего торгового счета на счет долевого инвестиционного управления, открытый Ф. для совершения сделок купли-продажи валют на международном рынке. Однако в процессе долевого инвестиционного управления денежными средствами у Ф. возник преступный умысел, направленный на хищение чужого имущества – вверенных ему денежных средств².

В данном случае к цифровым следам преступления относится информация с торговых счетов клиентов и счета долевого инвестирования.

Схема № 3 – хищение и незаконное использование логинов и паролей потерпевшего, необходимых для входа в личный кабинет последнего (рис. 3).



Рис. 3. Хищение денежных средств потерпевшего посредством предварительного хищения и незаконного использования его учетных данных от личного кабинета

В рассматриваемом случае хищение осуществляется посредством незаконного использования доступа к торговому счету и доступа к счетам третьих лиц, используемых для купли-продажи ценных бумаг.

Так, например К., получив информацию конфиденциального характера об имени, пароле, секретной и публичной части ключа криптографической защиты организации, принял заведомо незаконное решение получить, путем их противоправного использования, доступ к счетам и установить факт наличия ценного имущества или денежных средств. Во исполнение задуманного, К., используя личный компьютер, вошел через Интернет в информационно-торговую систему и получил доступ к счетам организации. Установив, что на ее счете-депо учтены права на бездокументарные ценные бумаги, у К. возник умысел на хищение чужого имущества.

Осознавая, что вероятность покупки ликвидных ценных бумаг организации по явно заниженной стоимости низка из-за возможности их приобретения добросовестными покупателями и что данные операции привлекут внимание организатора торгов и брокера, К. обратился к знакомым с требованием за вознаграждение открыть на

¹Приговор Октябрьского районного суда г. Самары от 3 сентября 2018 г. по делу № 1-64/18 // Сайт «Судакт» [Электронный ресурс]. Режим доступа: <https://sudact.ru/regular/doc/uXUWtVjRjJB/> (дата обращения: 06.09.2022).

²Приговор суда Ворошиловского района г. Волгограда от 10 апреля 2015 г. по делу № 1-8/15 // Сайт «Судакт» [Электронный ресурс]. Режим доступа: <https://sudact.ru/regular/doc/Avso89lDzsQw/?regular-txt=®ular-/> (дата обращения: 06.09.2022).

свои имена брокерские, депозитарные и банковские счета. Последние, не посвященные в преступные замыслы К., согласились и стали действовать по его указанию, передав ему доступ возможности от своего имени совершать сделки на рынке ценных бумаг и распоряжаться полученной прибылью. Кроме того, К. через этих же лиц внес на открытые ими счета личные денежные средства, необходимые для первоначального приобретения малоликвидных ценных бумаг со счета организации.

Реализуя задуманное, К. при помощи персонального компьютера (ноутбука) по сети Интернет, незаконно используя учетные данные и электронные ключи организации и своих знакомых, тем самым противоправно получили доступ к счетам организации.

Далее, незаконно действуя от имени организации, К. на торговой площадке ЗАО «Фондовая Биржа «ММВБ» осуществил несанкционированные операции по продаже ликвидных ценных бумаг, а также операции по покупке малоликвидных ценных бумаг с целью их дальнейшего использования для перевода денежных средств со счета организации на счет своих знакомых. К. совершал сделки купли-продажи с малоликвидными акциями, произведенными малыми пакетами, между, якобы, организацией и знакомыми, при которых продажа ценных бумаг от имени организации, умышленно осуществлялась по заниженной цене, а их последующая покупка от его же имени – по завышенной цене. В результате, активы организации снизились¹.

В данном случае к цифровым следам преступления относятся: информация с торгового счета организации и счетов третьих лиц.

¹Приговор Центрального районного суда г. Воронежа от 21 ноября 2014 г. по делу № 1-4/14 // Сайт «Судакт». URL: <https://sudact.ru/regular/doc/aZL79s4cjYVH/?regular-txt=®ular-> (дата обращения: 06.09.2022).

ЗАКЛЮЧЕНИЕ

Итак, в настоящее время все активнее в различных сферах деятельности используются цифровые технологии. Вместе с тем они нередко используются в преступных целях. Многие из преступлений рассматриваемой категории совершаются с применением информационных технологий, что обуславливает появление от них цифровых следов. Для борьбы с противоправными деяниями разработаны технологии изучения данных следов, которые могут присутствовать не только в Интернете, но и других информационных системах. Для выявления следов преступлений, совершенных с использованием возможностей межбанковского валютного интернет-рынка Форекс, необходимо анализировать информацию с сайтов и счетов потерпевших и подозреваемых.

Цифровыми следами от преступлений, совершенных с использованием компьютерной программы «Метатрейдер» или специально созданного сайта, является информация с сайта о котировках и их изменениях, о балансе электронных кошельков и движении денежных средств на них.

Цифровыми следами от преступлений, совершенных посредством хищения денежных средств инвесторов путем непредставления причитающихся им процентов от игры на интернет-рынке Форекс, является информация с торговых счетов и счета долевого инвестирования.

Цифровыми следами от хищения высоколиквидных акций потерпевшего посредством незаконного использования доступа к его торговому счету и торговым счетам третьих лиц, используемых «вслепую» для купли-продажи ценных бумаг, является информация с торговых счетов потерпевшего и третьих лиц.

СПИСОК ИСТОЧНИКОВ

1. Захарова В. О., Шкатулов К. О. О проблемах в ходе обнаружения, изъятия, использования цифровых следов в следственной деятельности // Вестник Московской академии Следственного комитета Российской Федерации. 2023. № 1. С. 68–74.
2. Романова Г. В. Информационные технологии в деятельности следователя // Вестник Волжского университета имени В. Н. Татищева. 2023. № 2. Т. 1. С. 159–168.
3. Буйнов О. Д. Виды цифровых следов преступлений в сфере экономической деятельности и особенности их исследования экспертом // Актуальные проблемы российского права. 2022. Т. 17. № 11 (144). С. 140–148.

REFERENCES

1. Zakharova, O. V. (2023). On the problems in the course of detection seizure use of digital traces in investigative activities. Bulletin of the Moscow Academy of the Investigative Committee of the Russian Federation, 1, 68–74. (In Russ.)

2. Romanova, G. V. (2023). Information technologies in the investigator's activity. Bulletin of the V. N. Tatishchev Volga State University, 2, 159–168. (In Russ.)
3. Buinov, O. D. (2022). Types of digital traces of crimes in the sphere of economic activity and features of their research by an expert. Actual problems of Russian law, 17, 11(144), 140–148. (In Russ.)

ИНФОРМАЦИЯ ОБ АВТОРЕ

Реуцкая Ирина Евгеньевна

кандидат психологических наук, доцент

ведущий научный сотрудник Всероссийского научно-исследовательского института

Министерства внутренних дел Российской Федерации

INFORMATION ABOUT THE AUTHOR

Reutskaya Irina Evgenyevna

PhD (Psychology), Associate Professor

leading researcher of All-Russian Research Institute

of the Ministry of Internal Affairs of the Russian Federation

Статья поступила в редакцию
одобрена после рецензирования
принята к публикации

21.01.2024
02.02.2024
16.02.2024

The article was submitted
approved after reviewing
accepted for publication